(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 January 2003 (30.01.2003)

PCT

(10) International Publication Number
WO 03/009513 A3

(51) International Patent Classification[7]: H04L 9/08, 9/28

(21) International Application Number: PCT/IL02/00571

(22) International Filing Date: 16 July 2002 (16.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
144369 17 July 2001 (17.07.2001) IL

(71) Applicant *(for all designated States except US)*: **KING GREEN LTD.** [IL/IL]; P.O. Box 321, 20 600 Moshava Yokneam (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **YANOVSKY, Eli** [IL/IL]; 9 Harduf Street, 34 747 Haifa (IL).

(74) Agent: **G. E. EHRLICH (1995) LTD.**; 28 Bezalel Street, 52 521 Ramat Gan (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

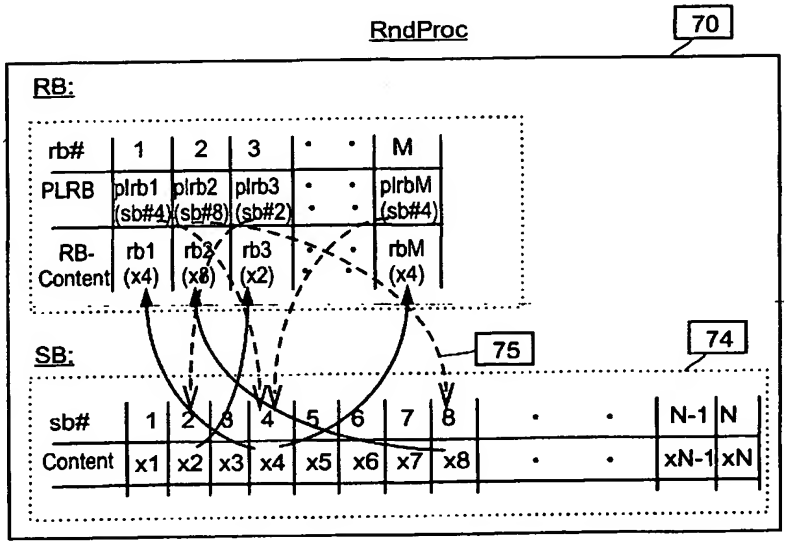
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
25 September 2003

[Continued on next page]

(54) Title: SECURE COMMUNICATION SYSTEM AND METHOD USING SHARED RANDOM SOURCE FOR KEY CHANGING



(57) Abstract: Apparatus for use by a first party for key management for secure communication with a second party, said key management being to provide at each party, simultaneously remotely, identical keys for said secure communication without transferring said keys over any communication link, the apparatus comprising: a datastream extractor (70), for obtaining from data exchanged between said parties a bitstream, a random selector (72) for selecting, from said bitstream, a series of bits in accordance with a randomization seeded by said data exchanged between said parties, a key generator (54) for generating a key for encryption/decryption (52) based on said series of bits, thereby to manage key generation in a manner repeatable at said parties.

WO 03/009513 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL02/00571

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L9/08; H04L9/28
US CL : 380/278
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/21, 28,30,46,49,278; 707/201; 375/356

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,375,169 A (SEHEIDT et al.) 20 December 1994 (20.12.1994), abstract, , Fig.3a, col. 5, line 56 throuigh col 6, line 2, col. 6, lines 14-67, col. 8, lines 31-52, see also claims 1 and 2...	1-4,19-23,37-39 --- 5-18,24-36,40-48
Y	5,923,758 a (KHAMHARA et al.) 13 July 1999 (13.07.1999), abstarct, Fig.,, col. 2, line 62 through col. 3, line18, Fig.2, col. 3, lines lines 19-67 , col. 5, line 39 through col. 6, line 27.	5-18, 24-36,40-48
Y,E	20020156798 A1 (LARUE et al.) 24 October 2002 (24.10.2002), the entire document)	5-18,24-36,40-48

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 January 2003 (29.01.2003)	03 MAR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Taghi T. Arani Telephone No. (703) 305-4274

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/IL02/00571

Continuation of B. FIELDS SEARCHED Item 3:
WEST , ProQuest, Dogpile: Serch terms: key adj management near5 randomi$6 and symetric adj key or split adj key and synchr$7, Key adj agreement